ABSTRACT

A method of encryption of data in a digital television system communicated between a first decoder and a portable security module, wherein a precalculated key pair is stored in a memory of the first decoder, wherein the key pair includes a session key and an encrypted version of the session key prepared using a transport key, the encrypted version of the session key being subsequently communicated to the portable security module which decrypts the encrypted version using an equivalent transport key stored in its memory such that data communicated from at least the portable security module to the first decoder may thereafter be encrypted and decrypted by the session key.